
UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA

: Hon. Mark Falk

v.

: Magistrate No. 18-3580 (MF)

ANKUR AGARWAL

: **CRIMINAL COMPLAINT**

I, David B. Madigan, the undersigned complainant being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this complaint is based on the following facts:

SEE ATTACHMENT B



David B. Madigan, Special Agent
Federal Bureau of Investigation

Sworn to before me and subscribed in my presence,
April 25, 2018
Newark, New Jersey

HONORABLE MARK FALK
UNITED STATES MAGISTRATE JUDGE



Signature of Judicial Officer

ATTACHMENT A

From in or about January 2018 to on or about April 19, 2018, in Somerset County, in the District of New Jersey, and elsewhere, defendant,

ANKUR AGARWAL

knowingly and intentionally accessed and attempted to access protected computers used in interstate and foreign commerce without authorization, and exceeded authorized access, and thereby obtained and attempted to obtain information from protected computers, the value of which information exceeded \$5,000, as described in Attachment B below, in violation of Title 18, United States Code, Sections 1030(a)(2)(C), (c)(2)(B)(i), and (c)(2)(B)(iii) and Section 2.

ATTACHMENT B

I, David B. Madigan, am a Special Agent of the Federal Bureau of Investigation. My experience as a Special Agent has included the investigation of computer crimes and other federal criminal violations of law. I have also received training and have gained experience concerning the investigation of cyber and computer investigations. I have knowledge of the facts set forth in this Criminal Complaint through my personal participation in this investigation and through oral and written reports from other federal agents, other law enforcement officers, and others. Where I assert that an event took place on a particular date, I am asserting that it took place on or about the date alleged. Statements of others described herein are set forth in substance and part. Since this Criminal Complaint is being submitted for a limited purpose, I have not set forth every fact that I know concerning this investigation; rather, I have only set forth those facts that I believe are sufficient to that show probable cause exists to believe that the defendant committed the offense set forth in Attachment A.

Background

1. At all times relevant to this Criminal Complaint:

a. A company located in New Jersey was a communications technology company that developed and provided, among other things, telecommunications infrastructure and services to the public (the "Victim Company"). The Victim Company developed and continues to develop a specific communications technology (the "Technology"). The Victim Company maintained computers and computer servers in New Jersey and elsewhere that were compromised during the criminal scheme described herein. The Victim Company maintained and used computers and computer networks in interstate and foreign commerce and communications in furtherance of its business activities.

b. Defendant Ankur Agarwal ("Agarwal"), a resident of Montville, New Jersey, was a former employee of the Victim Company. He left the company in or about March 2014. While employed with the Victim Company, defendant Agarwal worked as a network engineer. Defendant Agarwal was currently employed by another company engaged in the communications technology industry.

Overview of the Scheme to Unlawfully Access the Victim Company's Computer

2. In or about April 2018, after learning of suspicious network traffic on its computer network, the Victim Company identified malware¹ targeting its computer systems. According to the Victim Company, the malware attack demonstrated a high level of technical sophistication.

3. As part of its efforts to identify and mitigate the malicious computer activity, the Victim Company determined that some of the malicious network activity originated from one of the Victim Company's offices in New Jersey (the "New Jersey Office").

4. On or about April 18, 2018, personnel from the Victim Company discovered a hidden laptop computer (the "Laptop Computer One") inside the New Jersey Office. The Victim Company's personnel discovered Laptop Computer One concealed in a locked cabinet in an open cubicle (the "Cubicle"). At the time of discovery, Laptop Computer One was connected to the Victim Company's computer network. In addition, Laptop Computer One was connected to an external hard drive (the "Hard Drive"). Neither Laptop Computer One nor the Hard Drive belonged to the Victim Company. The Victim Company did not authorize any individual to connect Laptop Computer One to the company's computer network or to use Laptop Computer One to access the Victim Company's computer network. The Victim Company's personnel removed Laptop Computer One and the Hard Drive from the company's computer network, and both devices were secured.

5. On or about the morning of April 19, 2018, the Victim Company's personnel observed a male individual, wearing a hooded green jacket, physically present inside the New Jersey Office. This individual was physically present inside the New Jersey Office for approximately ten minutes. During that time and without authorization from the Victim Company, the individual connected a second laptop computer ("Laptop Computer Two") to the Victim Company's computer network. Thereafter, two security employees (the "Employees") from the Victim Company approached the individual. The individual then scuffled with one of the Employees and the individual fled on foot. According to the Victim Company, one of the Employees sustained a minor injury during the scuffle.

6. After this incident, the Victim Company contacted local law enforcement. The Victim Company also reviewed footage from its security cameras. This footage revealed this individual, wearing the hooded green jacket and a backpack (the "Backpack"), arriving at the New Jersey Office in a

1. Malware is malicious code or software that is intended to damage or disable computers and computer systems.

green Honda sedan and entering the premises by following behind another employee.

7. After arriving at the New Jersey Office, local law enforcement officers recovered the Backpack and Laptop Computer Two. The Backpack contained the following items and information, among other things:

- a. A luggage identification tag bearing the name "Ankur Agarwal" and his address in Montville, New Jersey;
- b. Legal papers in the name of defendant Agarwal and his wife;
- c. Tax papers in the name of defendant Agarwal; and
- d. A notebook (the "Notebook").²

8. Later that day, according to local law enforcement, an individual contacted the police department and reported that a green Honda sedan had been stolen. Based on the information described in Paragraph 6 above, police officers located defendant Agarwal in a nearby park in New Jersey and arrested him. At the police station, the Employees each identified defendant Agarwal as the same individual involved in the scuffle, as described in Paragraph 5 above.

9. According to the Victim Company, defendant Agarwal was neither authorized to be on the Victim Company's premises, including at the New Jersey Office, nor was he authorized by the company to access its computer network, including attaching hardware, downloading any content or information, or installing any code or software, such as hacking tools.

10. According to information from the Victim Company, the company identified a computer that had accessed, without authorization, its computer network. The Victim Company reported that this computer used a commercially available hacking framework (*i.e.*, a suite of hacking tools)(the "Hacking Tool Suite") to, among other things, expand unauthorized access to the Victim Company's computer network.

11. As part of this investigation, federal agents from the Federal Bureau of Investigation searched publically available information, including a website often used by computer engineers, programmers, and hackers (the "Website"). This search of open source information revealed that from in or about January 2018 through in or about March 29, 2018, defendant Agarwal

2. On or about April 20, 2018, federal agents executed a search warrant at defendant Agarwal's residence in Montville, New Jersey. Inside the residence, federal agents seized a second notebook. The handwriting in both notebooks is unique and appears substantially the same.

made several posting to the Website. For example, on or about March 29, 2018, defendant Agarwal posted an error message that he had received while using the Hacking Tool Suite. In this post, defendant Agarwal wrote: "Please see the error message when running exploit. It does not seem to get past authentication." In this post, defendant Agarwal set forth certain information, including computer commands, that he had used when attempting to gain access to a computer network. According to the Victim Company, some of the information in this post relates to certain internal and non-public information belonging to the Victim Company. Based on Your Affiant's education, training, and experience, I know the phase "get past authentication" refers to accessing a computer network, and therefore, defendant Agarwal's post relates to his attempt to remotely access, with a hacking tool, the Victim Company's computer network.

12. As part of this investigation, federal agents have reviewed the Notebook. The Notebook is handwritten and documents and logs computer activities conducted by defendant Agarwal on certain dates. For example:

a. On or about an entry dated April 3, 2018, defendant Agarwal documented, in detail, his attempts and success in exploiting the Victim Company's network. For example, defendant Agarwal noted after he had successfully penetrated Victim Company's network, the Victim Company's network monitoring team detected this intrusion and alerted the Victim Company. Defendant Agarwal noted in his Notebook that he had become aware of this alert. [Your Affiant asserts that defendant Agarwal became aware of this alert because he had accessed, without authorization, the Victim Company's network].

b. On or about an entry dated April 13, 2018, defendant Agarwal documented the status of an internal Victim Company investigation concerning a computer intrusion incident of the company's network. [Your Affiant asserts that defendant Agarwal obtained this information as a result of his unauthorized access to the Victim Company's network]. According to the Victim Company, the value of this information exceeds \$5,000.

13. Based on the above, Your Affiant asserts that probable cause exists to believe the following:

a. Defendant Agarwal was the individual who connected Laptop Computer One, Laptop Computer Two, and the Hard Drive to the Victim Company's computer;

b. The Victim Company did not authorize defendant Agarwal to connect, install, or attach any hardware, including Laptop Computer One, Laptop Computer Two, and the Hard Drive, to the Victim Company's computer network;

c. The Victim Company did not authorize defendant Agarwal to access the company's computer network, either at the New Jersey Office or remotely, and the Victim Company did not authorize defendant Agarwal to physically enter the New Jersey Office;

d. Defendant Agarwal gained unauthorized access onto the Victim Company's computer network and, as a result, acquired internal and non-public information belonging to the Victim Company.